Notice of Allowability	Application No.	Applicant(s)	
	09/936,315	SCHEIDT, EDWARD M.	
	Examiner	Art Unit	
	Longbit Chai	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *interview on 3/22/2006*.

2. ☒ The allowed claim(s) is/are *34-36*.

3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO-1449 or PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application (PTO-152)
6. ☒ Interview Summary (PTO-413), Paper No./Mail Date *3/22/2006* .
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

CHRISTOPHER REVAK
PRIMARY EXAMINER
3/26/06

DETAILED ACTION

Examiner's Amendment

An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Thomas M. Champagne (Reg. No. 36,478) on 3/22/2006.

This application has been amended as follows:

IN THE CLAIMS

Cancel claims 1 – 33 and claims 37 – 41.

Replace claim 34 as follows.

Claim 34: A method of establishing a secure communication channel, comprising:

sending, by a first party, a secure call notification to a second party;

accessing, by the first and second parties, base, prime, and sub-prime parameters;

generating, by the second party, a second asymmetric key pair comprising a second public key and a second private key, based on the base, prime, and sub-prime parameters;

sending, by the second party to the first party, the second public key;

generating, by the first party, a net label, a private label, a random value, a first asymmetric key pair comprising a first public key and a first private key based on the base, prime, and sub-prime parameters, and a shared key based on the second public key;

encrypting, by the first party, the net label, the private label, and the random value, using the shared key;

sending, by the first party to the second party, the encrypted net label, the encrypted private label, the encrypted random value, and the first public key;

generating, by the second party, the shared key based on the first public key;

decrypting, by the second party, the encrypted net label, the encrypted private label, and the encrypted random value using the shared key; and

exchanging, by the first and second parties, respective identification numbers to establish the secure communication channel;

~~The method of claim 33,~~ wherein the secure call notification is a first secure call notification, the net label is a first net label, the private label is a first private label, the random value is a first random value, the shared key is a first shared key, the encrypted net label is a first encrypted first net label, the encrypted private label is a first encrypted first private label, and the encrypted random value is a first encrypted first random value further, the method further comprising:

designating, by one of the first party and the second party, either of the first party and the second party as a sender, and the other of the first party and the second party as a non-sender;

suspending, by the sender, the secure communication channel between the first party and the second party;

establishing, by the sender, a communication channel with a third party;

sending, by the sender, a second secure call notification to the third party;

accessing, by the third party, the base, prime, and sub-prime parameters;

generating, by the third party, a third asymmetric key pair comprising a third private key and a third public key, based on the base, prime, and sub-prime parameters;

sending, by the third party to the sender, the third public key;

generating, by the sender, a second private label, a second net label, a second random value, a fourth asymmetric key pair comprising a fourth public key and a fourth private key based on the base, prime, and sub-prime parameters, and a second shared key based on the third public key;

encrypting, by the sender, the second private label, the first net label, and the first random value, using the second shared key, to provide an encrypted second private label, a second encrypted first net label, and a second encrypted first random value;

sending, by the sender to the third party, the encrypted second private label, the second encrypted first net label, the second encrypted first random value, and the fourth public key;

generating, by the third party, the second shared key based on the third public key;

decrypting, by the third party, the encrypted second private label, the second encrypted first net label, and the second encrypted first random value, using the second shared key;

suspending, by the sender, the secure communication channel between the sender and the third party;

sending, by the sender to the third party and the non-sender, a conference call notification;

encrypting, by the sender, the second net label and the second random value, using one of the first public key and the second public key, to provide a first encrypted second net label and a first encrypted second random value;

generating, by the sender, a first error detection value for the first encrypted second net label and the first encrypted second random value;

sending, by the sender to the non-sender, the first encrypted second net label, the first encrypted second random value, and the first error correction value;

generating, by the non-sender, a second error detection value, for the first encrypted second net label and the first encrypted second random value;

checking, by the non-sender, the validity of the first encrypted second net label and the first encrypted second random value by comparing the first and second error detection values;

decrypting, by the non-sender, the first encrypted second net label and the first encrypted second random value, using one of the first private key and the second private key;

encrypting, by the sender, the second net label and the second random value, using the third public key, to provide a second encrypted second net label and a second encrypted second random value;

generating, by the sender, a third error detection value, for the second encrypted second net label and the second encrypted second random value;

sending, by the sender to the third party, the second encrypted second net label, the second encrypted second random value, and the third error correction value;

generating, by the third party, a fourth error detection value, for the second encrypted second net label and the second encrypted second random value;

checking, by the third party, the validity of the second encrypted second net label and the second encrypted second random value by comparing the third and fourth error detection values; and

decrypting, by the third party, the second encrypted second net label and the second encrypted second random value, using third private key.

Allowable Subject Matter

1. Claims 34 – 36 are allowed.
2. The following is an examiner's statement of reasons for allowance:

The above mentioned claims are allowable over prior arts because the CPA (Cited Prior Art) of record fails to teach or render obvious the claimed limitations in combination with the specific added limitations, as recited in independent claim 34 and 35.

The prior arts (a) Chen , alone or in combination with Elgamal or (b) Gennaro, alone or in combination with Bjerrum, fail to teach or suggest a method for facilitating secure electronic communications among at least two parties over a communication network, comprising: establishing a communication link among at least three parties comprising a first party and other parties; sending, by the first party, a broadcast conference call notification to the other parties; accessing, by the first party and the other parties, base, prime, and sub-prime parameters; generating, by the first party, a net label, a random value, and a first asymmetric key pair comprising a first public key and a first private key based on the base, prime, and sub-prime parameters; sending, by the first party, the first public key to each of the other parties; generating, by each of the other parties, a respective private label, a respective other asymmetric key pair comprising a respective other public key and a respective other private key based on the base, prime, and sub-prime parameters, and a respective other shared key based on the first public key; encrypting, by each of the other parties, the respective private

label using the respective shared key; sending, by each of the other parties, the respective encrypted private label and the respective other public key to the first party; computing, by the first user, each respective shared key from each respective public key sent by the other parties; decrypting, by the first party, each respective encrypted private label using the respective shared keys.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Longbit Chai whose telephone number is 571-272-3788. The examiner can normally be reached on Monday-Friday 8:00am-4:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Longbit Chai
Examiner
Art Unit 2131

LBC LBC

CHRISTOPHER REVAI
PRIMARY EXAMINER
CR 3/26/06